Produt Overview

Celestix WSA Unified Access Gateway delivers ready-to-deploy, comprehensive, secure remote access to corporate resources for employees, partners, and vendors on both managed and unmanaged PCs and mobile devices. Utilizing a combination of connectivity options, ranging from SSL VPN to DirectAccess, as well as built in configurations and policies, WSA provides centralized and easy management of an organization's complete anywhere access offering.

Integrating a deep understanding of the applications published, the state of health of the devices being used to gain access, and the user's identity – Celestix WSA enforces granular access controls and policies to deliver comprehensive remote access, ensure security, and reduce management costs and complexity.

Celestix WSA Unified Access Gateway

The Comprehensive Solution for Secure Remote Access

Remote users often need to access network applications from private and public endpoints and through intermediate networks. Unsecured remote access threatens enterprises with the unauthorized disclosure of sensitive information left on endpoints and intermediate servers as well as with malicious attacks against the network and its applications from infected endpoint connections.

WSA™ SSL VPN appliances from Celestix™ with Microsoft® Forefront™ Unified Access Gateway 2010 (UAG) deliver secure, anywhere-access to messaging, collaboration, and other resources with granular control and world-class ease of deployment and management.

Control Access

Forefront UAG acts as a consolidated gateway from a diverse range of endpoints and locations to provide access through a single portal or multiple portals for different classes of users. Remote users—employees, partners, and customers—can access Web and non-Web applications and gain full VPN access to corporate networks including internal file shares and client/server applications. Strong, reliable authentication of all users keeps hackers out and speeds access for authorized users. Reliable authentication enables fine-grained control of access to network resources.

Comprehensive Secure Access

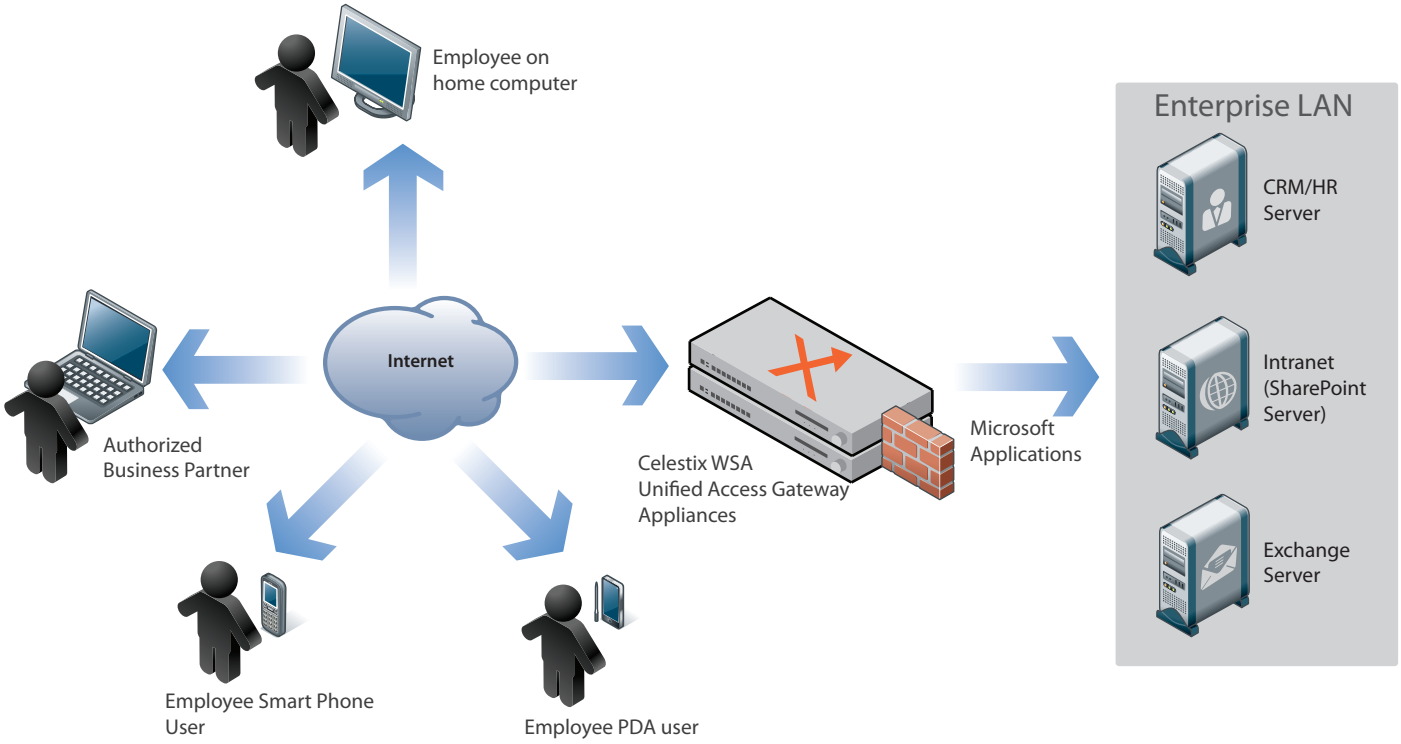
The WSA appliance provides SSL VPN, DirectAccess (always-on VPN), Application Optimizers, a Web application firewall, and endpoint security management that enable access control, authorization and content inspection for a wide variety of applications. These technologies provide mobile and remote workers with easy and flexible secure access from a broad range of devices and locations including kiosks, PCs, and mobile devices.

Enhance Compliance

Ensure that remote users comply with corporate security policies including endpoint configuration, user access, and accounting. Enforce compliance of different access policies for different user groups including classes of employees, business partners, and guests.

Protect Assets with Application Optimizers

WSA appliances host multiple intelligent Application Optimizers. Application Optimizers are integrated software modules that Microsoft designed to allow intelligent publishing of widely used business applications. This means you can choose to expose all or only selected areas of an application to all or subsets of users at your discretion. Application specific wipers check all interactions with the application for a wide range of threats and exploits. Application Optimizers amply support Microsoft client/server applications including Exchange Server, SharePoint Portal Server and Internet Information Server. Application Optimizers also support many third-party applications such as Citrix, SAP, IBM Domino, WebSphere and Lotus Notes.



Connectivity

WSA has four connectivity modes to provide the exact access your users and security standards require.

Web Applications

You can publish applications that provide a web user interface directly through WSA. The gateway can present a single application site, or offer a portal that lets users select multiple applications from a menu. The gateway offers the benefit of single sign-on and intelligent scanning of traffic to exclude malware. Secure Sockets Layer cryptography protects all applications.

Client/Server

Client/Server applications operate transparently through the UAG gateway with the added protection of an SSL VPN connection to prevent exposure of confidential information to the Internet. The UAG gateway maps internal addresses and ports so that no information about the internal network can leak out. UAG also provides intelligent application optimizers that scan for application-specific attacks. Strong authentication, single sign-on and fine-grained access policies ensure that only authorized users are allowed controlled access. You can set access control based on endpoint type and location as well as by user type. For example, a policy may dictate different access rights from a corporate PC than from a smart phone or public kiosk. Session cleanup with cache purging ensures that no confidential information will remain on a public computer after the authorized user logs off.

DirectAccess

Progressive businesses that want to provide their remote users with “always on” access should consider DirectAccess. The Windows® 7 and Windows Server® 2008 R2 operating systems include DirectAccess, which allows remote users to securely access enterprise shares, Web sites, and applications without connecting to a virtual private network (VPN). DirectAccess treats all endpoints as if they are on your internal network. The benefit is that Active Directory group policies, security updates and patch management can all be enforced directly on the connected client. DirectAccess support is built-in to Celestix WSA appliances and can bridge the transition between traditional SSL VPN remote access and fully DirectAccess-enabled networks. The WSA enhances Direct Access by extending support to older legacy business applications and non-windows clients within your network.

Network Connector

Some users and applications require unencumbered access. Network Connector provides network-level connections to the entire internal network or to a restricted subnet defined by the access policy. Network Connector supports all Microsoft resource sharing protocols such as CIFS, NET-Bios, and LDAP.

An SSL VPN without Vulnerabilities

Many SSL VPN implementations tunnel past the corporate firewall and expose the internal network to external threats. WSA incorporates Microsoft Forefront Unified Access Gateway 2010 and Microsoft Forefront Threat Management Gateway 2010 into a single integrated security appliance. By combining SSL VPN and firewall functions, the WSA appliance ensures that the VPN cannot be a backdoor past the firewall and into the enterprise network. All SSL VPN sessions must also pass all firewall rules.

A single WSA appliance can present multiple gateways to the external world. You can implement logically separate gateways for E-mail, partner extranets, and any number of other functions in a single WSA appliance. WSA provides the most cost effective implementation in terms of the number of appliances required and in ease of management since you can manage multiple gateways from a single console. You can also configure a single WSA appliance to present a portal with multiple applications to the user. You can configure WSA gateways to meet your enterprise's specific secure access needs.

Securing the Perimeter

UAG, with Intelligent Application Optimizers, provides network separation and full control of inbound and outbound content. The integrated WSA appliance provides the most advanced edge security protection to address a broad range of Internet threats. Combining stateful packet filtering, circuit filtering, application-layer filtering, Web proxy, and endpoint security into a single appliance affords the administrator the broadest range of options to enable policy-compliant access to applications and network resources.

Product Features

Scalability	
Users	Supports a vast number of users on a single gateway.
High Availability	Scales linearly with up to 8 appliances (using NLB) and up to 50 appliances (using an external load balancer, such as the Celestix CLB).
Manageability	
Flexibility	Delivers out-of-the-box configurations for widely deployed enterprise applications and customization capabilities including: authentication, authorization and endpoint compliance profiles, and context-sensitive Web portals. Supports positive logic rule sets and URL filter customization. Has the ability to develop rule sets for customized or proprietary applications.
SSL VPN Portal	Enables a convenient single access point for applications, yet supports multiple access points with distinct policy parameters such as partner extranets and employee portals on a single gateway.
Logging and reporting	Supports monitoring, logging and reporting for enterprise-level management and accounting (system, user security, and session views): • Event Monitor provides comprehensive event monitoring by user, application, and time period • Integrated Event Logger records system usage and user activities and sends alerts about security events to an administration console. • Integrated Event Query tool with preconfigured query templates and full reporting capabilities.
Comprehensive policy framework	• Out-of-the-box application access settings and endpoint policy configurations designed to ensure minimal integration overhead and low ongoing management costs. • Supports Intelligent Application Toolkit for defining positive logic rule sets, URL filters to supplement Optimizer settings and to develop policies for customized or proprietary applications. • Supports Intelligent Application Template that provides a framework to build an Application Optimizer for both generic Web applications and complex enterprise applications incorporating components, web parts and objects.
Access Policy	
Endpoint compliance checks	Endpoint policy allows administrators to define compliance checks according to out-of-the-box variables including presence of security software and UAG-specific components such as Attachment Wiper. Supports complex endpoint policy rules with customizable compliance checks using Boolean operations.
End user experience	• Delivers a standard SSL VPN portal and login pages to enable easy set up and low administrative overhead. • Supports comprehensive portal and login page customization to replicate existing intranet. Does not require conformance to a vendor portal template.
Included Application Optimizers	Microsoft SharePoint Portal Server, Microsoft Exchange Server, Microsoft Dynamics, and more.

Technical Specifications

WSA 3200

500 users

- 1U 19" Rack-mountable
- Core 2 Duo Processor
- 4GB of 667MHz DDR2 SDRAM
- 1066MHz frontside bus
- 300GB available storage 7,200-rpm Serial ATA-II hard drive
- Six Gigabit Ethernet NIC
- Three USB 2.0 ports
- One 9-pin serial port
- One RJ-45 serial port
- AC Power Voltage 100-240VAC, 50-60Hz with power switch and temperature-controlled fan
- Dimensions: 1.75" (H) x 16.9" (W) x 12.25" (D)

WSA 4200

500-1,000 users

- 1U 19" Rack-mountable
- Intel® Core 2 Duo processor
- 4GB of 667MHz DDR2 SDRAM
- 1333MHz frontside bus
- Six Intel Gigabit Ethernet NIC
- Three USB 2.0 ports
- Two 9-pin serial console ports
- Two 7,200-rpm Serial ATA-II hard drives in RAID 1 configuration, 120GB available storage
- AC Power Voltage 100-240VAC, 50-60Hz with power switch and temperature-controlled fan
- Dimensions: 1.75" (H) x 17.3" (W) x 12.25" (D)

WSA 6200

4,000 users

- 1U 19" Rack-mountable
- Intel® i5-660 processor
- 8GB of DDR3 SDRAM
- Six Gigabit Ethernet NIC
- Three USB 2.0 ports
- One 9-pin serial console port
- Two hot swappable 7,200-rpm Serial ATA-II hard drives in RAID 1 configuration, 300GB available storage
- Redundant hot swappable 250W power supplies with PFC (RoHS compliant)
- Dimensions: 1.75" (H) x 17.3" (W) x 15.6" (D)

WSA 8200

15,000 users

- 2U 19" Rack-mountable
- Dual Quad-Core Intel® Xeon® (Nehalem) processors
- 12GB of 667MHz DDR3 SDRAM ECC Registered
- Eight Intel Gigabit Ethernet NIC (PCIe)
- Four hot swappable 7,200-rpm 160GB Serial ATA-II hard drives in RAID 5EE configuration 300GB available storage
- Redundant hot swappable 550W power supplies with PFC (RoHS compliant)
- Dimensions: 3.5" (H) x 17.4" (W) x 26.0" (D)

Panel Display

- Front Panel Jog Dial (Power Button)
- 40 x 2 Character LCD Display
- Power LED, HD Activity, Alert LED
- VGA Console

Safety and Emissions Certifications

- Safety: ENC 55022:1998 + A1:2000 + A2:2003 Class B, EN61000-3-2:2000 + A1:2001 + A2:2005, EN61000-3-3:1995 + A1:2001 + A2:2005, IEC 61000-4-2:1995 +A1:1998 + A2:2001, IEC 61000-4-3:1995 +A1:1998 + A2:2002, IEC 61000-4-4:1995 +A1:2001 + A2:2001, IEC 61000-4-5:1995 +A1:2001, IEC 61000-4-6:2004, IEC 61000-4-8:2001, IEC 61000-4-11:2004
- Emissions: FCC Class B, CE, CB, C-Tick and RoHS.

Order Information

Microsoft requires all UAG client systems to have a Client Access License (CAL). Customers with qualifying CALs/ECALs do not need to purchase CALs individually.

WSA 3200	
WSA-12111-010	WSA 3200 Unified Access Gateway Appliance
WSA 4200	
WSA-12113-010	WSA 4200 Unified Access Gateway Appliance
WSA 6200	
WSA-12115-010	WSA 6200 Unified Access Gateway Appliance
WSA 8200	
WSA-92604-010	WSA 8200 Unified Access Gateway Appliance
External Connector	
WSA-EC123-000	External Connector for Celestix WSA

Please contact our sales representative or authorized reseller for support options.

For more information about WSA appliances, contact Celestix today at:

Americas	+1 510 668.0700
United Kingdom	+44 (0) 118 959 6198
Singapore	+65 6781.0700
India	+91 44 3910 3530

440 Mission Court
Suite 231
Fremont, California 94539

©2011 Celestix Networks Inc. All Rights Reserved. Celestix, WSA and Celestix logo are trademarks of Celestix Networks, Inc. All other products and company names mentioned are trademarks or registered trademarks of their respective owners.

Part number: DS-WSAUK-05